ICTACADEMY

TATA STRIVE | Right Skills Bright Future

Introduction to Cyber Security

Understanding Threats, Attacks Categories, Hacking Processes

Feb 2021

TATA TRUSTS

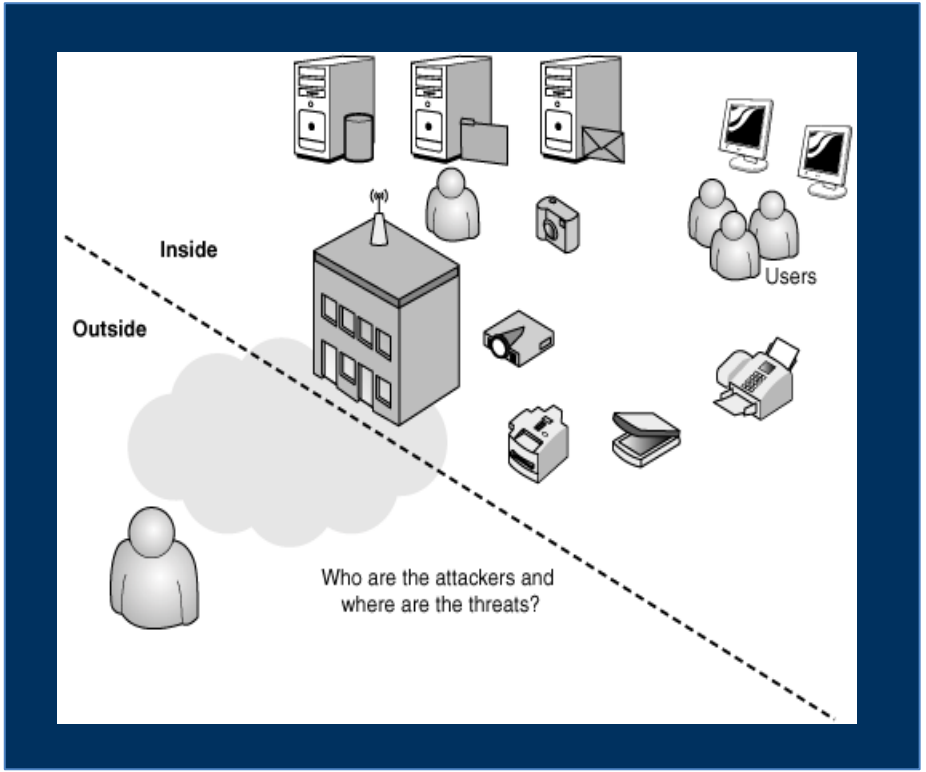
What are Internal and External Threats?

Created by fae frey
from Noun Project

A threat can be caused by:

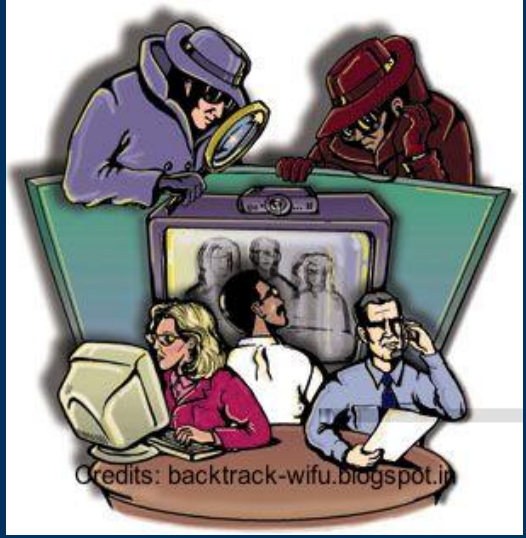
Internal Threat

External Threat

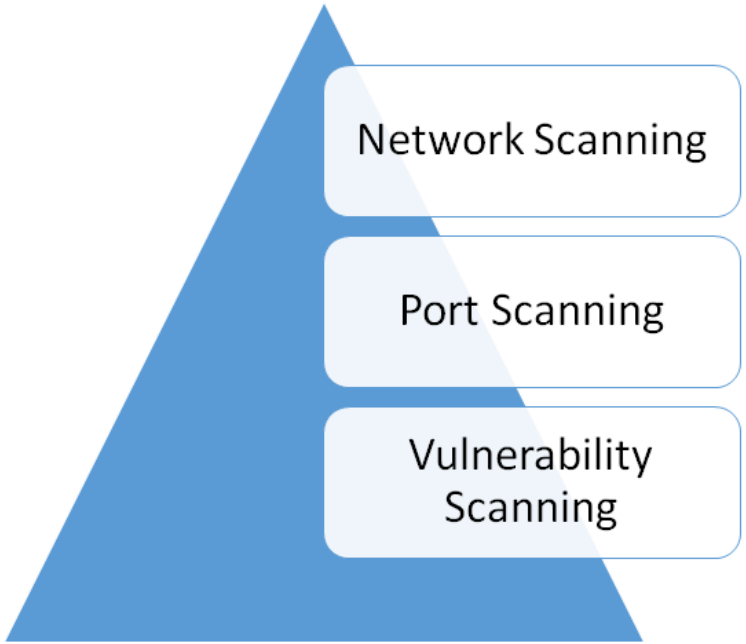


Reconnaissance helps to:

- Know Security Posture
- Reduce Attack Area
- Identify vulnerabilities
- Draw Network map



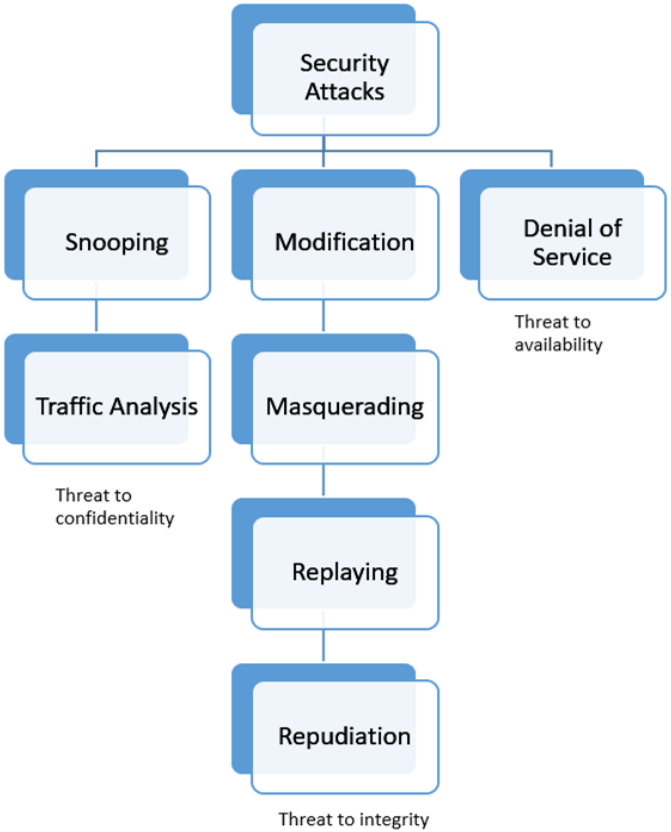
Scanning is a set of procedures for identifying live hosts, ports, and services, discovering Operating system and architecture of target system, Identifying vulnerabilities and threats in the network.

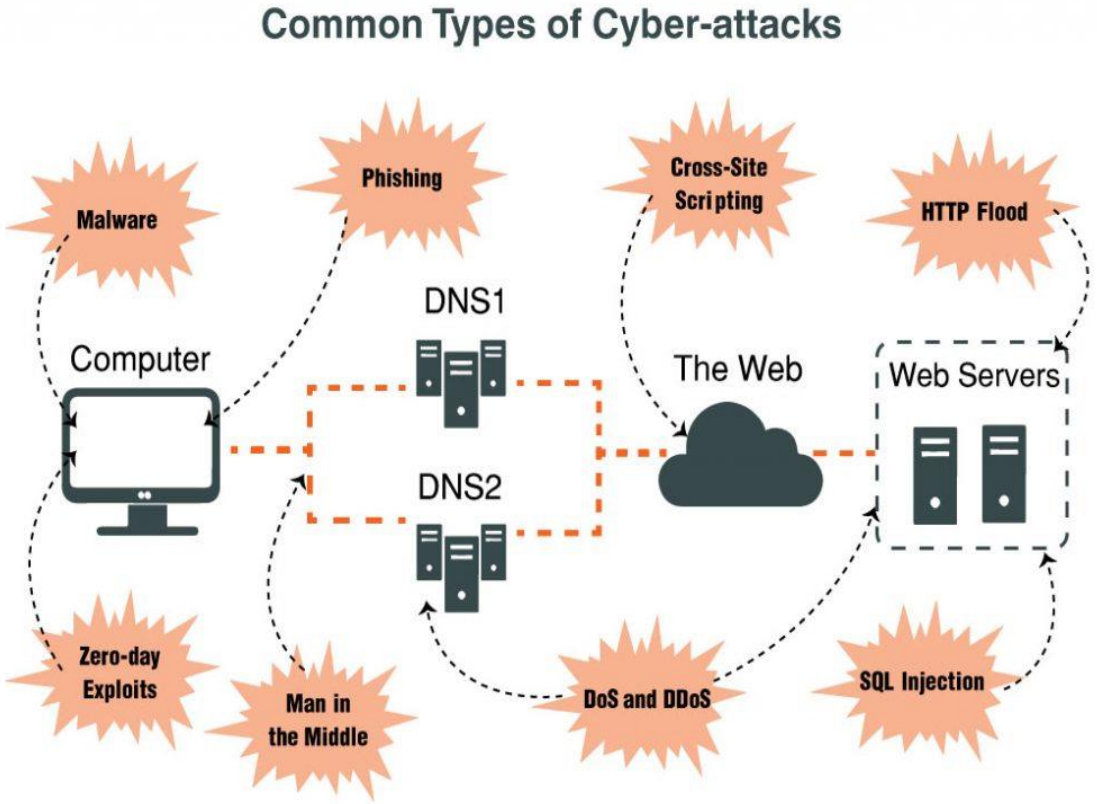


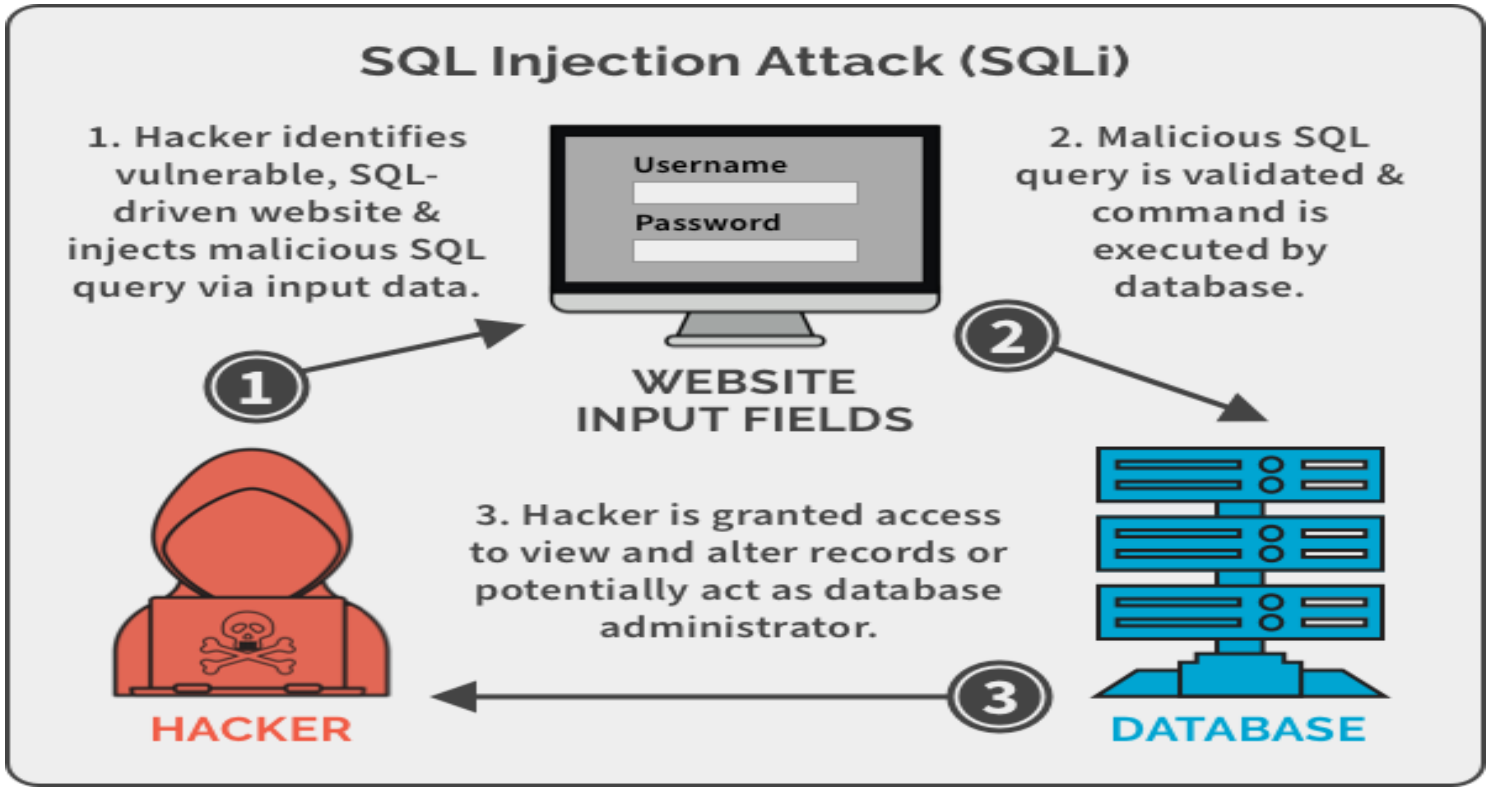
What is a Cyber Attack?

Created by fae frey
from Noun Project

Different Attacks




Common Types of Cyber-attacks
Malware
Phishing
Cross-Site Scripting
HTTP Flood
DNS1
Computer
The Web
Web Servers
DNS2
Zero-day Exploits
Man in the Middle
DoS and DDoS
SQL Injection



Source: Spanning Backup

SQl Example

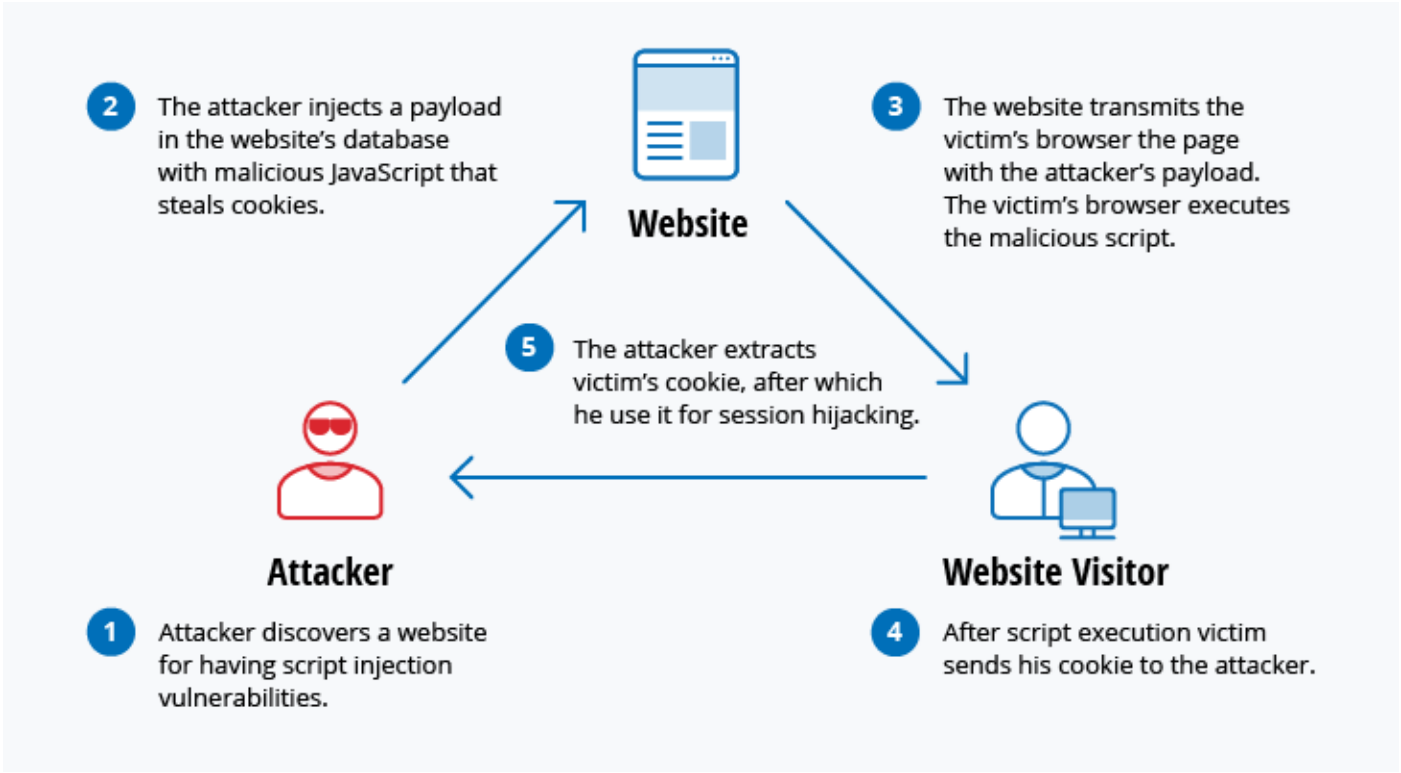
A web form on a website might request a user's account name and then send it to the database in order to pull up the associated account information using dynamic SQL like this:

```
"SELECT * FROM users WHERE account = '" + userProvidedAccountNumber +"';"
```

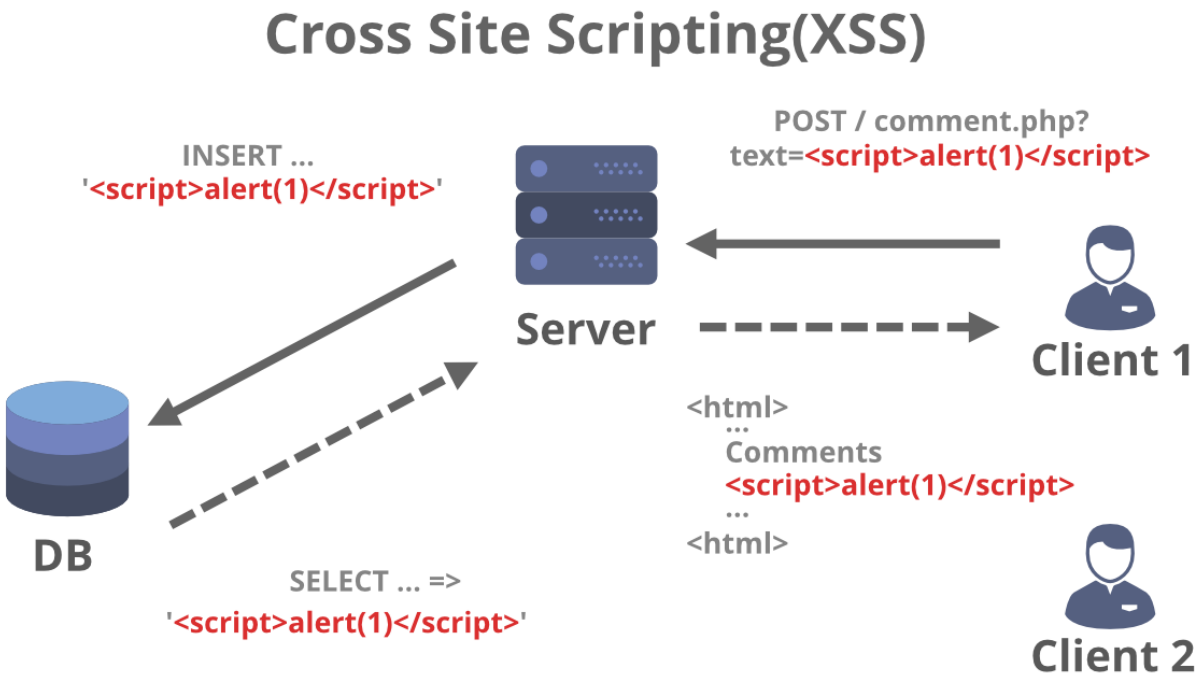
While this works for users who are properly entering their account number, it leaves a hole for attackers. For example, if someone decided to provide an account number of *"' or '1' = '1'"*, that would result in a query string of:

```
"SELECT * FROM users WHERE account = '' or '1' = '1';"
```

Because *'1' = '1'* always evaluates to TRUE, the database will return the data for all users instead of just a single user.


2
The attacker injects a payload in the website's database with malicious JavaScript that steals cookies.
Website
3
The website transmits the victim's browser the page with the attacker's payload. The victim's browser executes the malicious script.
5
The attacker extracts victim's cookie, after which he use it for session hijacking.
Attacker
Website Visitor
1
Attacker discovers a website for having script injection vulnerabilities.
4
After script execution victim sends his cookie to the attacker.

Cross Site Scripting Example



Source: Geeks for Geeks

Drive-by Download Attack

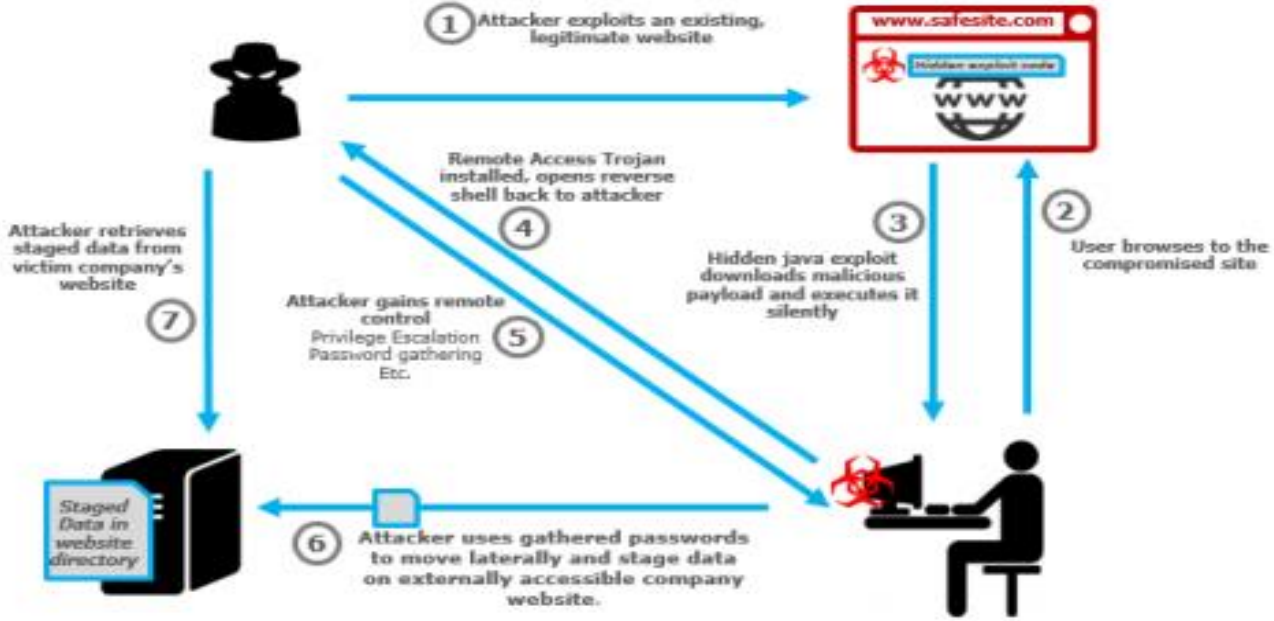
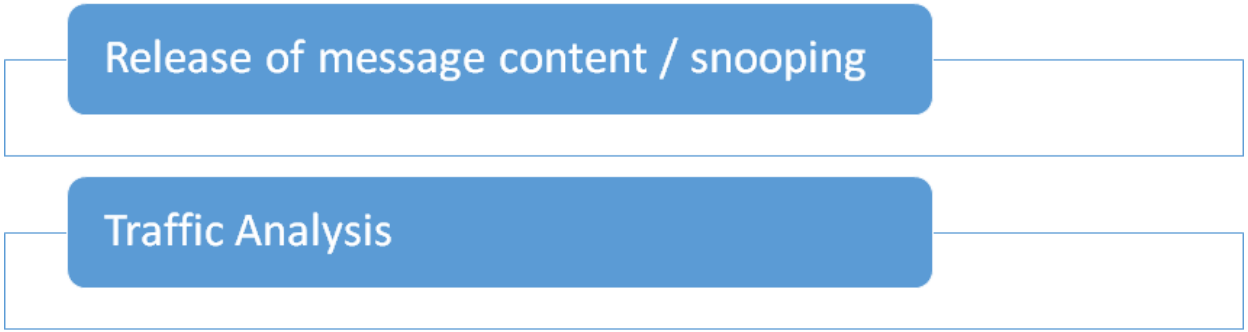


Figure 1 - Typical sequence of events in a drive-by download attack

Passive attack (emphasis on prevention rather than detection): Passive attacks are in the nature of eavesdropping on, or monitoring of, transmissions. The goal of the opponent is to obtain information that is being transmitted. Two types of passive attacks are:



Name of the Activity

Taboo

Instructions

Mode: **In-session**

Duration: **5 minutes**

Materials Required: **None**

Active attacks (involves some modification): Active attacks involve some modification of the data stream or the creation of a false stream and can be subdivided into four categories:

- Masquerade
- Replay
- Modification of messages
- Denial of Service

Name of the Activity

Behind the Door Number

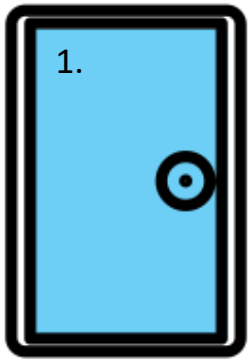
Instructions

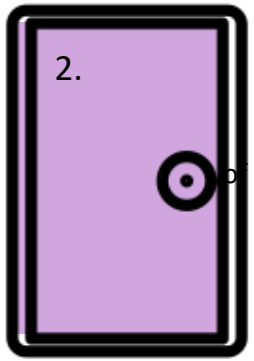
Mode: **In-session**

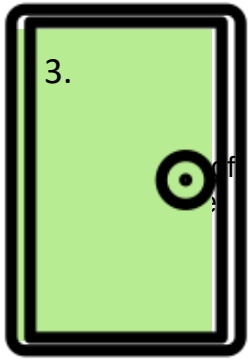
Duration: **5 minutes**

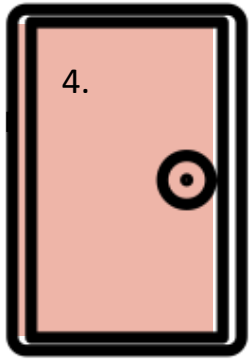
Materials Required: **None**

Knowledge Check – Behind the Door Number









Source: Noun project

Tasks of vulnerability assessment are the following:

Classifying the Vulnerabilities

- Hardware Vulnerability
- Software Vulnerability
- Network Vulnerability
- Physical Vulnerability
- Organization Vulnerability

Name of the Activity

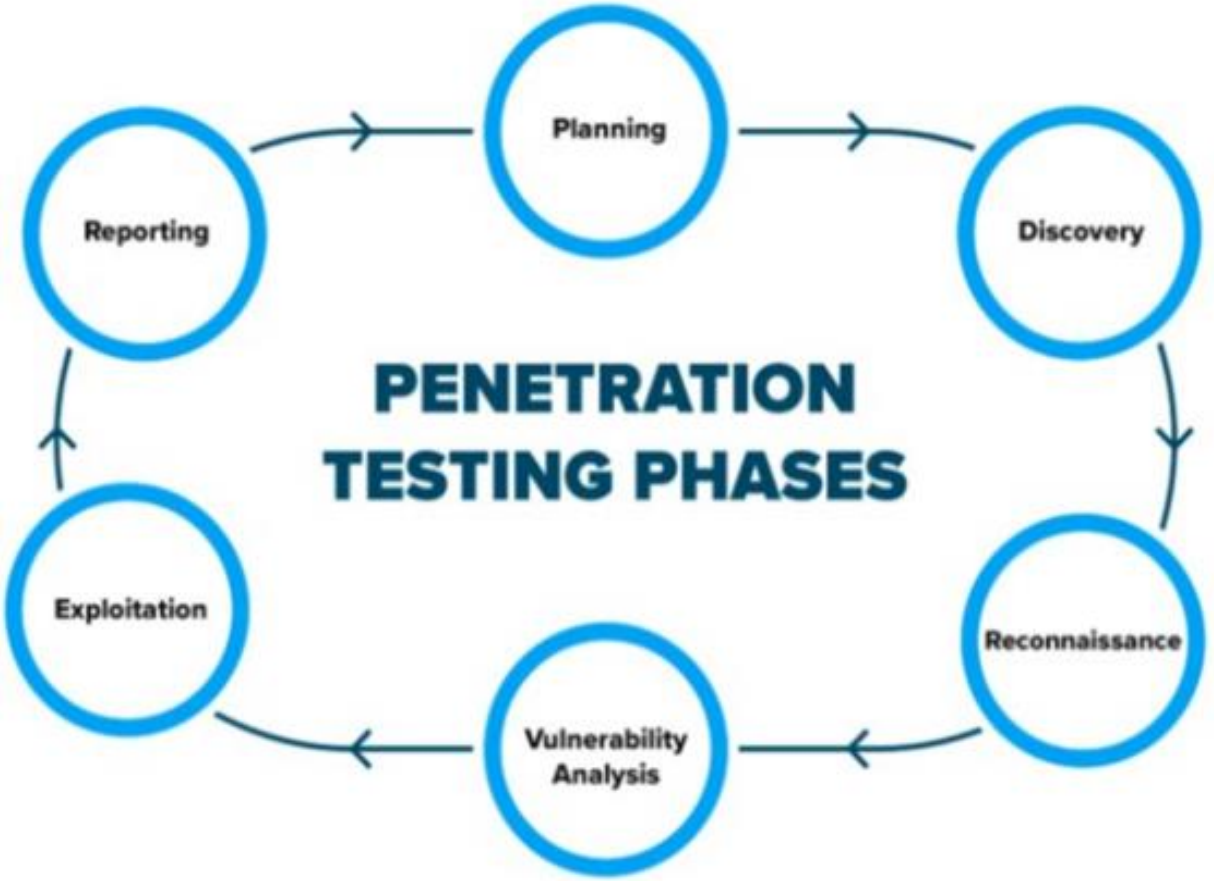
Taboo

Instructions

Mode: **In-session**

Duration: **5 minutes**

Materials Required: **None**


Planning
Discovery
Reconnaissance
Vulnerability Analysis
Exploitation
Reporting
PENETRATION TESTING PHASES

Name of the Activity

Complete the Image

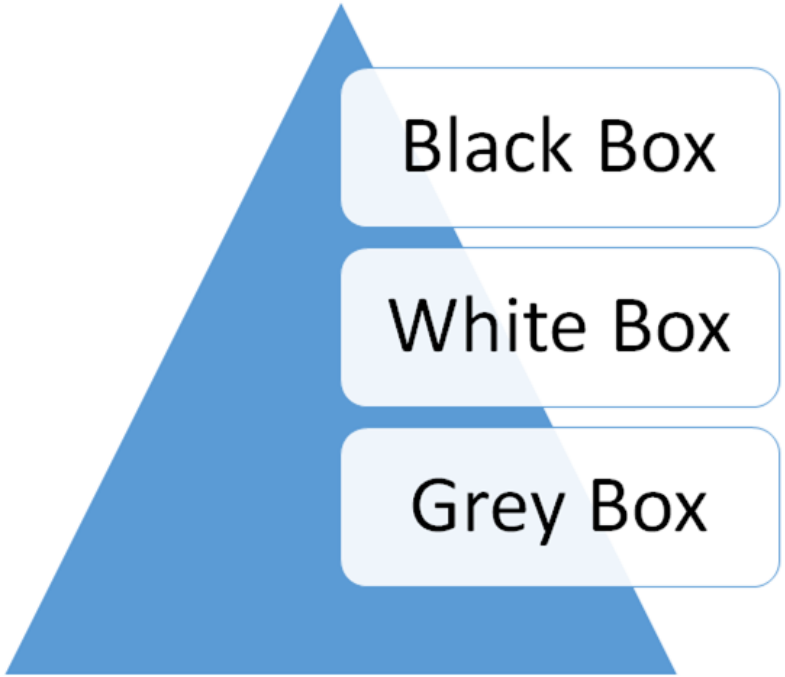
Instructions

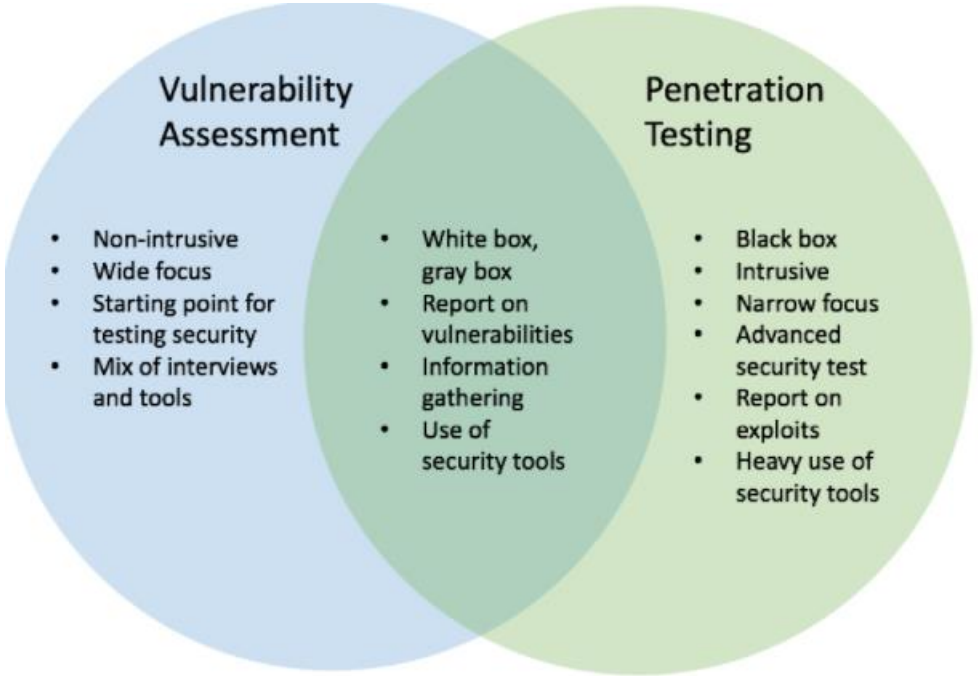
Mode: **Jamboard**

Duration: **5 minutes**

Materials Required: **None**

Jamboard Link:
https://jamboard.google.com/d/1orSKhcwiXO0BdoX8G91I2PEkl-ElsYWUIr_LBYiH4a0/edit?usp=sharing


Black Box
White Box
Grey Box


Vulnerability Assessment
Non-intrusive
Wide focus
Starting point for testing security
Mix of interviews and tools
White box, gray box
Report on vulnerabilities
Information gathering
Use of security tools
Penetration Testing
Black box
Intrusive
Narrow focus
Advanced security test
Report on exploits
Heavy use of security tools

Name of the Activity

Face Off

Instructions

Mode: **In-session**

Duration: **5 minutes**

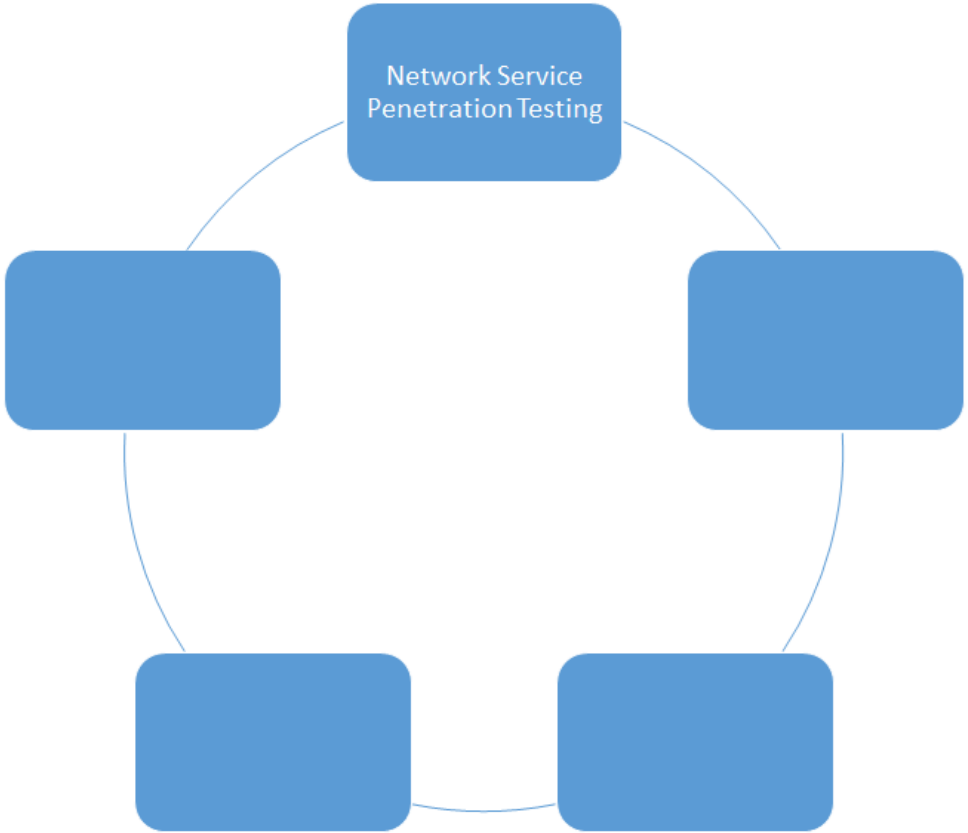
Materials Required: **None**

White Box Penetration Testing
v/s
Black Box Penetration Testing

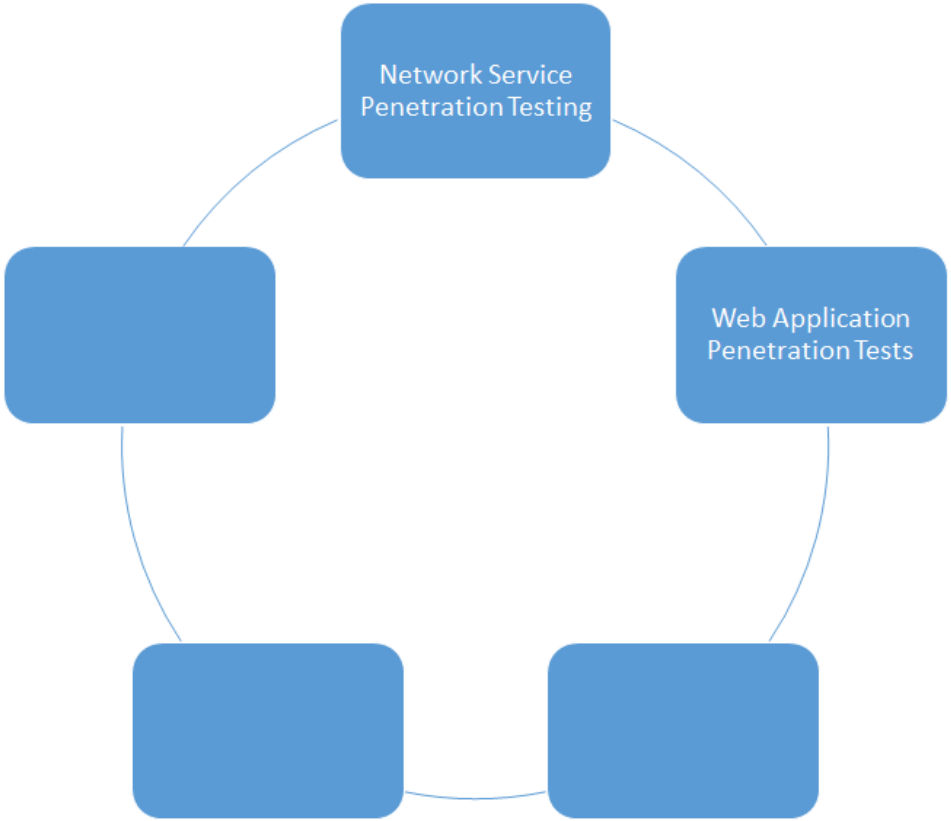
Why Conduct a Penetration Test?

Five Types of Penetrations Test

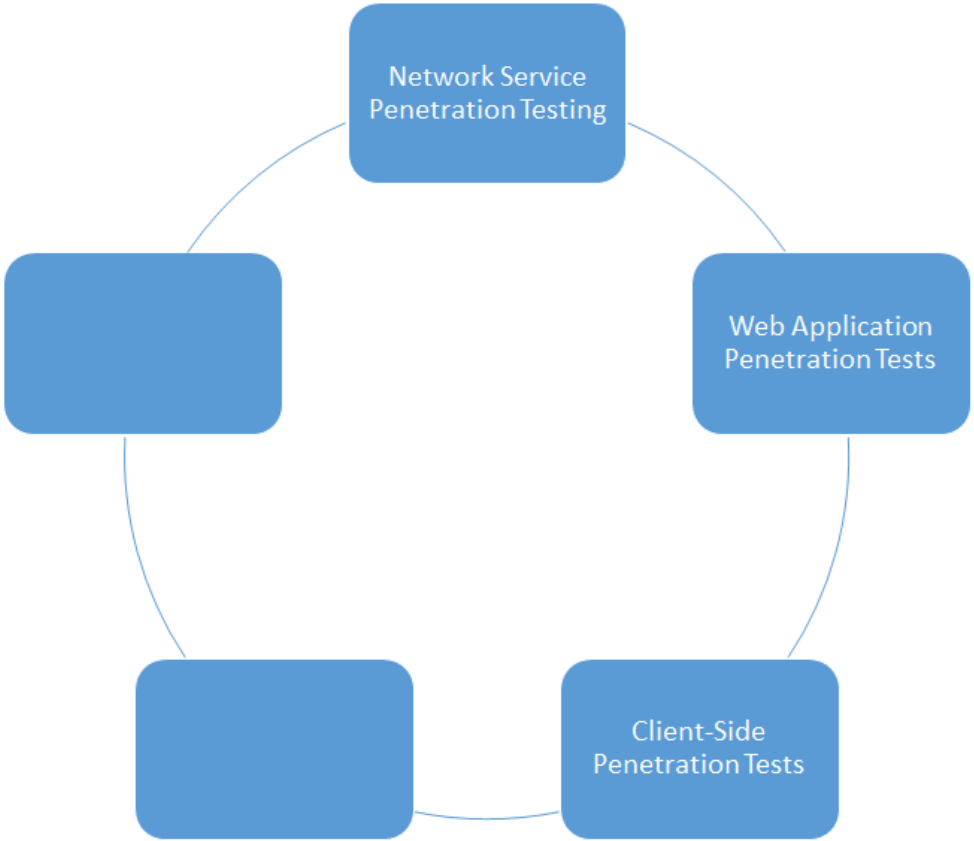
Five Types of Penetrations Test



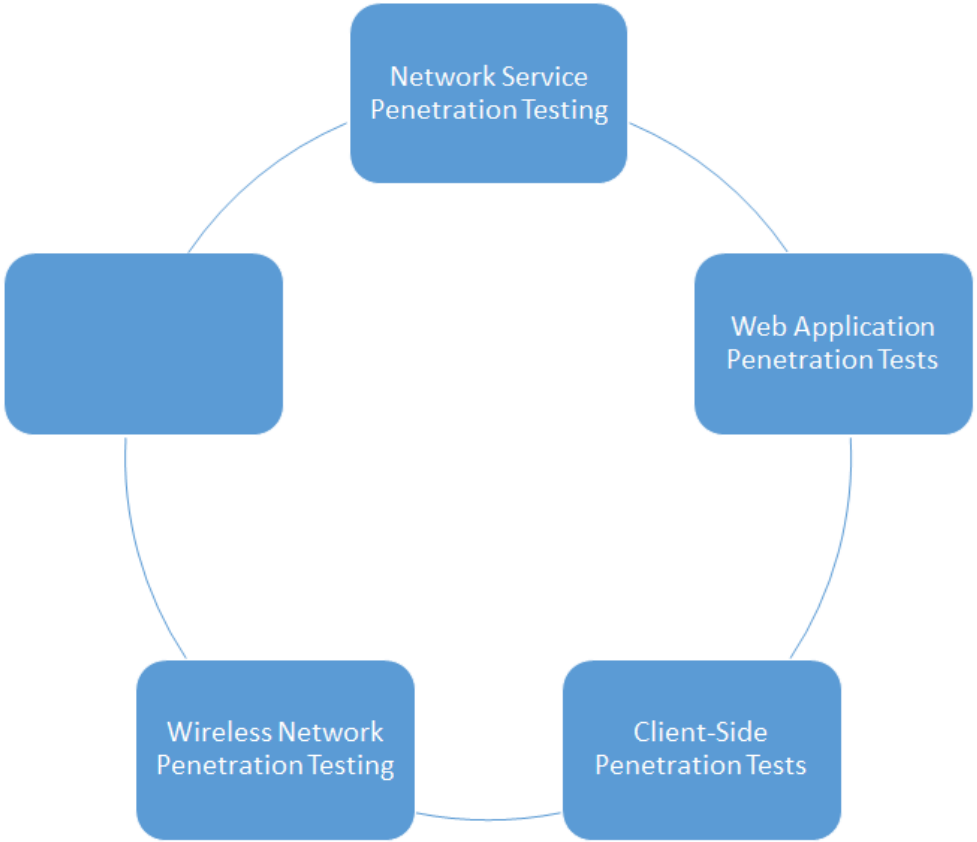
Five Types of Penetrations Test



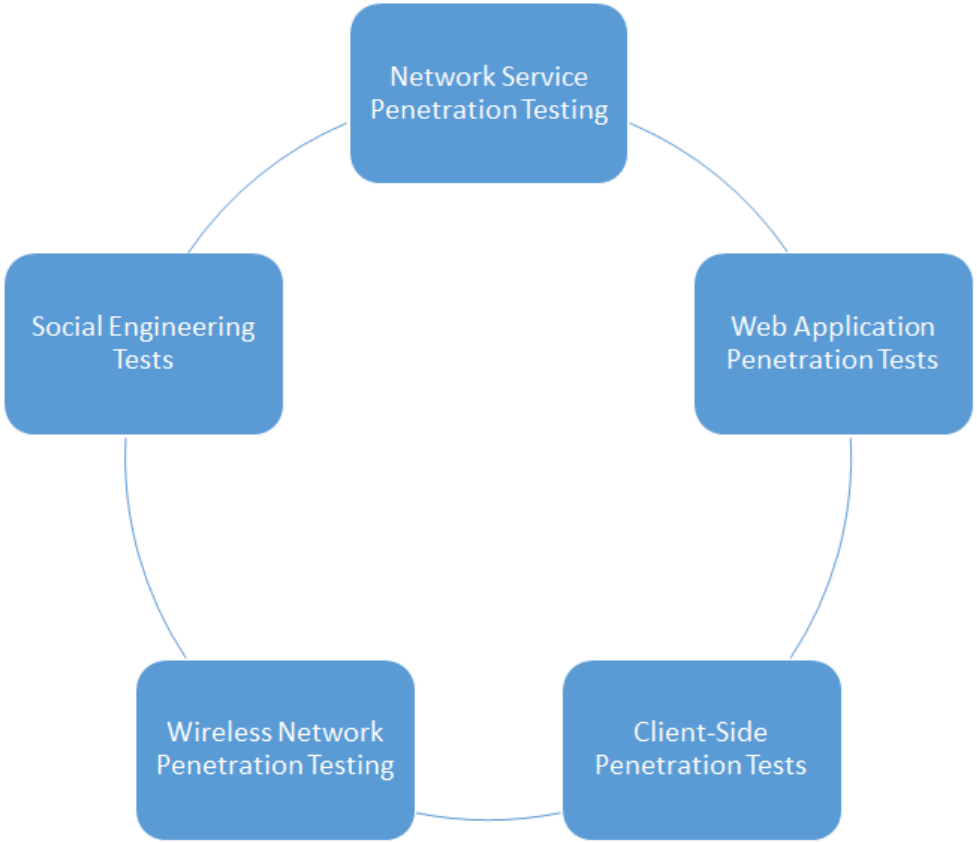
Five Types of Penetrations Test



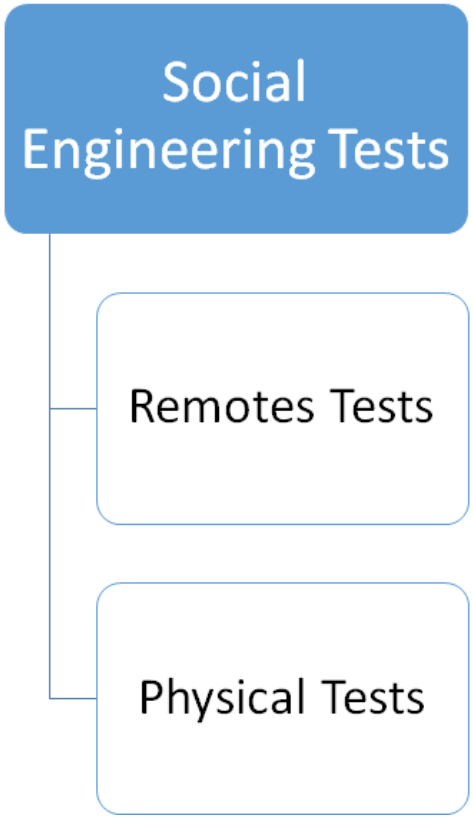
Five Types of Penetrations Test



Five Types of Penetrations Test



Subcategories of Social Engineering Tests



Name of the Activity

Who am I?

Instructions

Mode: **In-session**

Duration: **5 minutes**

Materials Required: **None**

Activity – Who am I?

1. Masquerade and Denial of Service are classified under what? **Active Attacks**

2. In which type of scanning are different tools used to identify the services or applications that are running on those systems? **Port Scanning**

1. Name the two types of Passive Attacks. **Release of message content/snooping and Traffic Analysis**

2. During a _____ penetration test, the pen tester has partial knowledge or access to an internal network or web application. **Grey Box**

3. The goal of _____ tests is to pinpoint security threats that emerge locally. **Client Side**

4. Name the two subcategories of Social Engineering Tests **Remote and Physical**

Summary

In this session, you learnt about:

- Fundamentals of Reconnaissance
- Fundamentals of Scanning & Methodology
- Different types of attacks
- Vulnerability Assessment
- Penetration Testing